IN THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the Application:

LISTING OF CLAIMS:

1. (Canceled)

2. (Previously Presented) A method of generating an identity authentication code associated with an authentication device, comprising:

providing event state data that specifies an operating condition of the authentication device, the operating condition specifying information on the likelihood that the authentication device has or will develop an operational problem; and,

generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device.

3. (Previously presented) The method of claim 2, wherein the identity authentication code further depends on a dynamic value.

4. (Previously presented) The method of claim 3, wherein the dynamic value includes one or more of a time value, a challenge, and a counter.

Claim 5 (Canceled).

6. (Previously Presented) The method of claim 2, further including changing the event state data when the operating condition of the authentication device changes.

7. (Previously Presented) The method of claim 2, wherein the operating condition of the device is covertly encoded in the identity authentication code.

8. (Previously presented) The method of claim 2, wherein the event state data is derived from an associated event secret.

9. (Previously presented) The method of claim 8, further including periodically changing the event secret.

10. (Previously presented) The method of claim 8, further including changing the event secret each time the dynamic value changes.

11. (Currently Amended) The method of claim ~~5~~26, further including changing the event secret when the security indicator of the authentication device changes.

12. (Previously presented) The method of claim 2, wherein the event state data includes one or more event state bits, a subset of bits being employed in generating identity authentication codes for different time intervals.

Claim 13 (Canceled).

14. (Previously Presented) The method of claim 2, wherein the operating condition of the authentication device includes information about whether a battery supplying power to the authentication device has fallen below an expected power level.

Claim 15 (Canceled).

16. (Previously Presented) The method of claim 2, wherein the operational problem is a device reset.

17. (Previously presented) The method of claim 2, wherein the identity authentication code further depends on of one or more of a PIN, a password, data derived from a biometric observation, user data, verifier data, and a generation value.

18. (Previously presented) The method of claim 2, further including, before generating the authentication code, receiving user input data, wherein the user input data is at least one of a PIN, a password, and biometric data.

19. (Previously presented) The method of claim 18, further including, before generating the authentication code, verifying whether the user input data is correct, and providing the identity authentication code only if the user input data is verified to be correct.

20. (Previously presented) The method of claim 2, further including transmitting the identity authentication code to a verifier.

21. (Previously presented) The method of claim 20, further including receiving, by the verifier, authentication information comprising the identity authentication code; and,

determining, by the verifier, the correctness of the identity authentication code and the event state data.

22. (Previously presented) The method of claim 20, wherein the verifier includes a representation of the secret associated with the device.

23. (Previously presented) The method of claim 21, wherein the authentication information further includes a user identifier.

24. (Previously Presented) The method of claim 21, wherein the authentication information further includes at least one of a PIN, a password, and biometric data.

25. (Previously presented) The method of claim 2, further including the step of displaying the identity authentication code on the device.

26. (Currently Amended) A method of generating an identity authentication code associated with an authentication device, comprising:

providing event state data that is a security indicator for an authentication system of which the authentication device is a component; ~~and,~~

generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device; and

generating the event state data using a funkspiel scheme;

wherein the security indicator includes information about whether the device has been subjected to tampering.

27. (Previously presented) The method of claim 26, wherein the identity authentication code further depends on a dynamic value.

28. (Previously presented) The method of claim 27, wherein the dynamic value includes one or more of a time value, a challenge, and a counter.

29. (Previously presented) The method of claim 26, wherein the security indicator includes information regarding strength of a biometric match,

30. (Previously presented) The method of claim 26, wherein the security indicator includes information regarding accuracy of a PIN entry.

31. (Previously presented) The method of claim 26, wherein the security indicator includes information regarding a device type associated with the authentication device.

32. (Previously presented) The method of claim 26, wherein the security indicator includes information regarding a device signature or pattern associated with the authentication device.

33. (Currently Amended) ~~The method of claim 26,~~ A method of generating an identity authentication code associated with an authentication device, comprising:

providing event state data that is a security indicator for an authentication system of which the authentication device is a component; and,

generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device;

wherein the security indicator includes information regarding a length of time the authentication device has been inserted into a device reader.

34. (Currently Amended) ~~The method of claim 26,~~ A method of generating an identity authentication code associated with an authentication device, comprising:

providing event state data that is a security indicator for an authentication system of which the authentication device is a component; and,

generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device;

wherein the security indicator includes information regarding a protection level of the secret associated with the device.

35. (Previously presented) The method of claim 26, wherein the identity authentication code further depends on one or more of a PIN, a password, data derived from a biometric observation, user data, verifier data, and a generation value.

36. (Previously presented) The method of claim 26, further including, before generating the authentication code, receiving user input data, wherein the user input data is at least one of a PIN, a password, and biometric data.

37. (Previously presented) The method of claim 36, further including, before generating the authentication code, verifying whether the user input data is correct, and providing the identity authentication code only if the user input data is verified to be correct.

38. (Previously presented) The method of claim 26, further including transmitting the identity authentication code to a verifier.

39. (Previously presented) The method of claim 38, further including receiving, by the verifier, authentication information comprising the identity authentication code; and,

determining, by the verifier, the correctness of the identity authentication code and the event state data.

40. (Previously presented) The method of claim 38, wherein the verifier includes a representation of the secret associated with the device.

41. (Previously presented) The method of claim 39, wherein the authentication information further includes a user identifier.

42. (Previously presented) The method of claim 39, wherein the authentication information further includes at least one of a PIN, a password, and biometric data.

Claims 43-56 (Canceled).

57. (Currently Amended) A method of generating an identity authentication code associated with an authentication device, comprising:

providing event state data that specifies information about environmental conditions associated with the authentication device; and,

generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device;

wherein the temperature characteristics include an ambient temperature to which the authentication device is exposed.

58. (Previously presented) The method of claim 57, wherein the identity code further depends on a dynamic value.

59. (Previously presented) The method of claim 58, wherein the dynamic value includes one or more of a time value, a challenge, and a counter.

Claim 60 (Canceled).

61. (Currently Amended) The method of claim ~~60~~57, wherein the temperature characteristics include an ambient temperature to which the authentication device is exposed.

62. (Currently Amended) The method of claim ~~60~~57, wherein the temperature characteristics include a temperature of a component of the authentication device.

63. (Currently Amended) ~~The method of claim 57,~~ A method of generating an identity authentication code associated with an authentication device, comprising:

providing event state data that specifies information about environmental conditions associated with the authentication device; and,

generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device;

wherein the information includes radiation levels to which the authentication device has been exposed.

64. (Currently Amended) ~~The method of claim 57,~~ A method of generating an identity authentication code associated with an authentication device, comprising:

providing event state data that specifies information about environmental conditions associated with the authentication device; and,

generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device;

wherein the information indicates whether static discharge to the device has occurred.

65. (Previously presented) The method of claim 57, wherein the identity authentication code further depends on one or more of a PIN, a password, data derived from a biometric observation, user data, verifier data, and a generation value.

66. (Previously presented) The method of claim 57, further including, before generating the authentication code, receiving user input data, wherein the user input data is at least one of a PIN, a password, and biometric data.

67. (Previously presented) The method of claim 66, further comprising, before generating the authentication code, verifying whether the user input data is

correct, and providing the identity authentication code only if the user input data is verified to be correct.

68. (Previously presented) The method of claim 57, further including transmitting the identity authentication code to a verifier.

69. (Previously presented) The method of claim 68, further including receiving, by the verifier, authentication information comprising the identity authentication code; and,

determining, by the verifier, the correctness of the identity authentication code and the event state data.

70. (Previously presented) The method of claim 68, wherein the verifier includes a representation of the secret associated with the device.

71. (Previously presented) The method of claim 69, wherein the authentication information further includes a user identifier.

72. (Previously presented) The method of claim 69, wherein the authentication information further includes at least one of a PIN, a password, and biometric data.

73. (Previously Presented) A method for verifying the correctness of an identity authentication code, comprising:

receiving authentication information including the identity authentication code generated by an authentication device that depends on (i) a secret associated with the device, and (ii) event state data that specifies an operating condition of the authentication device, the operating condition specifying information on the likelihood that the authentication device has or will develop an operational problem;

verifying the correctness of the identity authentication code, and determining the condition of the authentication device in response to the received identity authentication code.

74. (Previously presented) The method of claim 73, further including taking an action in response to the event state.

75. (Previously presented) The method of claim 73, further including determining whether an event occurred in response to the determined event state.

Claim 76 (Canceled).

77. (Previously presented) The method of claim 73 wherein the condition of the device is covertly encoded in the authentication code.

78. (Previously presented) The method of claim 73, wherein the authentication information further includes a user identifier.

79. (Previously presented) The method of claim 78, wherein the authentication information further includes at least one of a PIN, a password, and biometric data.

80. (Previously presented) The method of claim 73, wherein the verifying the correctness of the identity authentication code further includes generating an expected identity authentication code that depends an expected event state data.

81. (Previously presented) The method of claim 73, wherein the verifying the correctness of the identity authentication code further includes recovering the event state data from the identity authentication code.

82. (Previously presented) The method of claim 80, wherein the event state data includes one or more event state bits, a subset of bits being employed in generating identity authentication codes for different time interval.

83. (Currently Amended) A method for verifying the correctness of an identity authentication code, comprising:

receiving authentication information including the identity authentication code generated by an authentication device that depends on (i) a secret associated with the device, and (ii) event state data that is a security indicator for an authentication system of which the authentication device is a component; and

verifying the correctness of the identity authentication code, and determining the event state data in response to the received identity authentication code;

wherein the security indicator includes information about whether the device has been subjected to tampering; and

wherein the event state data was generated using a funkspiel scheme.

Claim 84 (Canceled).

85. (Currently Amended) A method for verifying the correctness of an identity authentication code, comprising:

receiving authentication information including an identity authentication code generated by an authentication device that depends on (i) a secret associated with the device, and (ii) event state data that specifies information about environmental conditions associated with the authentication device; and

verifying the correctness of an identity authentication code, and determining the event state data in response to the received identity authentication code;

wherein the information includes temperature characteristics associated with the authentication device.

86. (Currently Amended) The method of claim ~~5~~26, wherein:

a first secret and a second secret are stored within the authentication device;

the event state data encodes a first state or a second state, the first state indicating that no tampering has occurred, and the second state indicating that tampering has occurred;

wherein, if the event state data encodes the first state:

the secret associated with the device is the first secret; and

generating an identity authentication code includes cryptographically combining the first secret with a dynamic value; and

wherein, if the event state data encodes the second state:

the secret associated with the device is the second secret; and

generating an identity authentication code includes cryptographically combining the second secret with a dynamic value.

87. (Previously Presented) The method of claim 30, wherein the method further includes:

if the security indicator indicates that the PIN of a user using the authentication device has been entered incorrectly more than a specified number of times, then restricting access of the user by eliminating the user's access to highly confidential information, while permitting access to non-confidential information.

88. (New) The method of claim 83 wherein the security indicator further includes information regarding a length of time the authentication device has been inserted into a device reader.

89. (New) The method of claim 83 wherein the security indicator further includes information regarding a protection level of the secret associated with the device.

90. (New) The method of claim 85 wherein the temperature characteristics include an ambient temperature to which the authentication device is exposed.

91. (New) The method of claim 85 wherein the temperature characteristics include a temperature of a component of the authentication device.

92. (New) The method of claim 85 wherein the information further includes radiation levels to which the authentication device has been exposed.

93. (New) The method of claim 85 wherein the information indicates whether static discharge to the device has occurred.